
BUILD YOUR
IT SECURITY
BUSINESS CASE.
The challenge, the solution and
how to get the business on board.
With Kaspersky, now you can.
kaspersky.com/business
Be Ready for What's Next
KASPERSKY lab

BUSINESS DRIVERS AND THEIR IMPACT ON IT.

1

At Kaspersky Lab, we know that businesses are under pressure and they all face the same key challenges to stay afloat: they need greater agility, better efficiency and improved productivity. To help meet these challenges, companies are turning to IT to improve processes, deploy and support new systems and technology and of course manage and protect an ever growing amount of corporate data.

But what's the impact of this on you and your team? And in a tough economic climate how do you manage these challenges with limited resources and budget while ensuring your business achieves its goals?

Executive summary

The technology used by today's 'average' business has become increasingly complex.

Business in general is ever more reliant on technology and the internet – with company data needing to be accessed, shared and used more quickly and by a greater diversity of employees, suppliers and customers.

Mobility is the most often cited business trend that has transformed the way many of us work and communicate.

From an IT security perspective, this means that protection methods and tools from even a few years ago are rapidly becoming 'unfit for purpose'.

Whilst most IT professionals recognise this, it's an unfortunate fact that most businesses fail to prioritise the investments that are needed to create an approach that's both robust and adaptable to changing needs and the fast-paced nature of everything in business.

Recognising these challenges, this guide looks at the business arguments for evolving and improving IT security.

This guide provides crucial facts to assist you in building a robust business case, meeting the demands of your business and protecting against threats now and in the future.

WHY READ THIS GUIDE?

- Get key facts and statistics to help you develop a robust business case for IT Security
- Find out more about security risks and how to combat them
- Find out how new integrated security platforms help productivity whilst delivering endpoint security
- Find out more about how Kaspersky can help you close the gaps in your security posture and reduce the number of tools you have to work with.

TODAY'S DYNAMIC BUSINESS USING YESTERDAY'S IT SECURITY?

2

Mobile devices, remote workers, removable media, third party applications, web applications…All great for productivity, but if you're an IT Security professional, just another potential vulnerability.

Traditional defences no longer work

Anti-malware on its own is no longer enough to cope with the diversity and volume of threats your business is facing.

It's not just the older technology that's feeling the strain: 58 per cent of companies admit their IT security is under-resourced in at least one area of staff, systems or knowledge.[1]

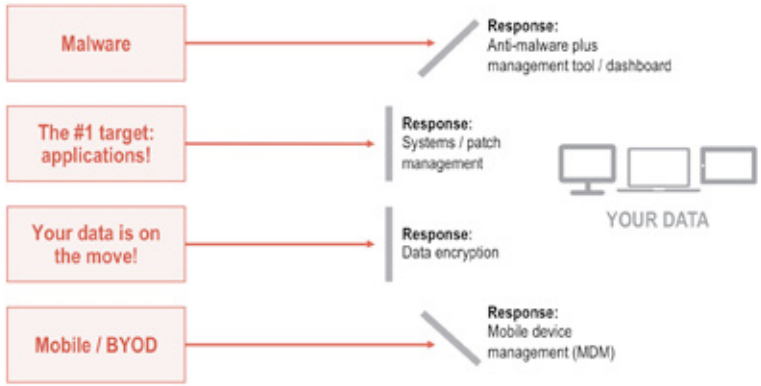
If you're in IT Security, chances are you're either running just to stand still or you're struggling to get the support you need to keep up with the threats. Or maybe you're juggling an ever-growing array of disparate solutions (see fig 1) – each with its own console, user interface and maintenance requirements. Never mind the compatibility issues you have to deal with.

Business is increasingly adopting new technologies without considering the security implications. While some businesses are adequately prepared, many are not, providing further incentive, if any were needed, for the ever more sophisticated and organised hackers, malware and spyware developers, and spammers.

THE RESULT?

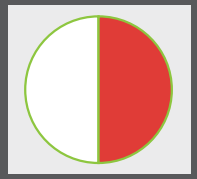
You're chasing your tail, reacting to change and assessing risk after technology has been adopted while trying to protect your business.

Fig 1: Disparate solutions each with their own console

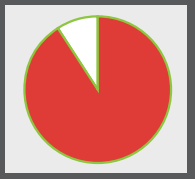


DID YOU KNOW?

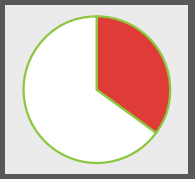
50% OF BUSINESSES VIEW CYBER THREATS AS A CRITICAL RISK TO THEIR ORGANISATION[1]



91% OF ORGANISATIONS HAVE HAD A DIRECT CYBER-ATTACK IN THE LAST YEAR[1]



35% OF ORGANISATIONS HAVE EXPERIENCED SEVERE DATA LOSS[1]



1. Source: Kaspersky Lab – Coping in the chaos Global IT Risk Report 2012

So, how can a Unified Endpoint Platform change this?

Unified Endpoint Platforms (also known as EPP) can help take the pain out of the complexity you face.

It's likely you've already invested in a fairly robust anti-virus solution but you should consider the broader risks and how to protect against them. These risks range from patching holes in applications to protecting data on laptops and securing mobile devices.

The core challenge in today's environment isn't that there are no tools available, it's that each individual tool adds to the complexity you face when trying to implement your security policies. And as you are aware complexity is the enemy of IT security.

By integrating security capabilities with systems management tools, EPP allows you to use a single console to manage your growing security needs.

Robust control tools, encryption systems and mobile device management can all be controlled from one place – while keeping anti-malware protection at the core of everything that happens on your network.

EPP gives IT Security professionals an easy way to manage costs, increase performance, lower their resource footprint and centralise management (see fig 2).

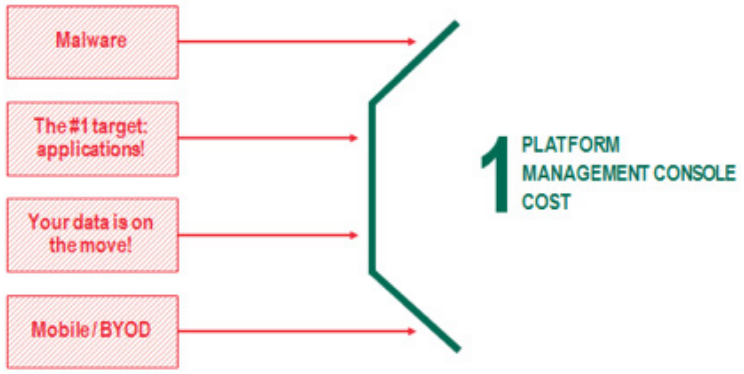
Deep integration can also underline system security and stability.

A note of caution

There's a big difference between 'integration' and a genuine platform. And when it comes to integration, there are varying degrees of completeness. For many, 'integration' has become just another word for 'compatible.'

Genuine platforms allow you to leverage the complementary strengths of each of the other components – giving you an overall solution that's greater than the sum of its parts.

Fig 2



UNIFIED ENDPOINT PLATFORM BENEFITS

- A Unified Endpoint Platform will make it easy for you to see your risk across your systems and endpoints.
- Enabling you to apply your policies consistently.
- Bringing your security posture in line with your business objectives.
- One Platform, One Console, One Cost.
- So you're able to reduce the risk to your data, reduce the complexity of your security tools, and reduce your investment whilst delivering against business demands.

MOBILITY, BYOD AND HYPER-CONNECTIVITY… LET'S LOOK AT THE RISKS.

4

So, what are the real risks? Technology sprawl, limited resources and lack of business understanding of many security issues are just the tip of the iceberg…

Mobility, mobile devices, device and application diversity

Smart devices are driving productivity, but they also bring new threats.

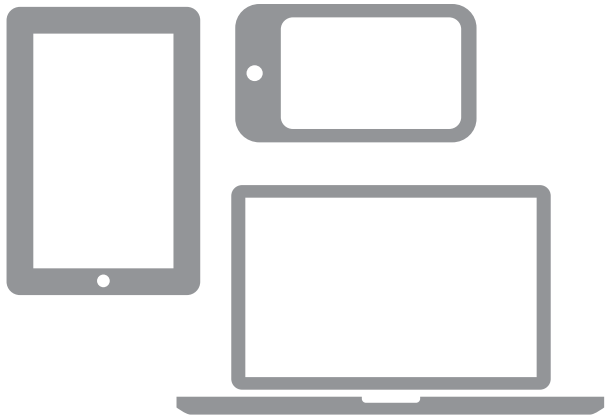
The average information worker now uses three devices – that's more for you to manage and control, and more opportunities for data loss, malware attack and ever growing complexity.

Employees are bringing personal devices into the workplace, with or without your permission – and often misplacing them along with your sensitive company data.

The BYOD trend is particularly popular with senior personnel and you not only have to cope with securing lost devices but also with employees wanting to access the company network and company information. This can lead to IT losing the battle for control.

Globally, 44% of companies allow staff uncontrolled connectivity to the network and corporate resources using a notebook with 33% permitting this via a smartphone[1].

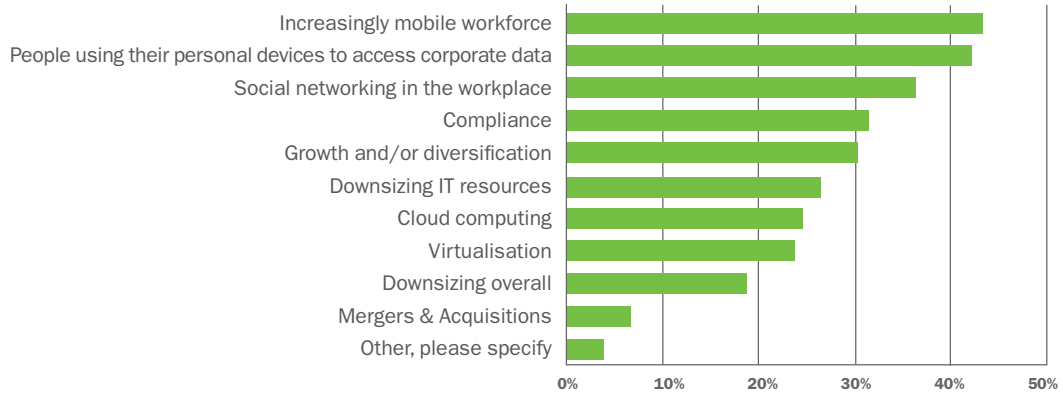
In March 2012, Kaspersky conducted a piece of global research in conjunction with analysts Bathwick Group 'Security readiness in a changing technology landscape' which found that mobility is currently the top area of concern for IT professionals around the world (see fig 3).



AT A GLANCE

- BYOD adds to complexity – the average employee uses three devices
- 44% of companies allow staff uncontrolled connectivity to the network and corporate resources using a notebook
- Mobility is currently the top area of concern for IT professionals around the world

Fig 3: What challenges are creating the biggest security headaches for your organisation?[1]



1. Source: Kaspersky Lab – Coping in the chaos Global IT Risk Report 2012

5

Rather than trying to prevent BYOD, the focus is now on finding a way to manage it.

When employees are using mobile devices the business sees increased productivity, cost-efficiency and flexibility but the reality for the IT Security team is different.

Business benefits can quickly become IT security challenges - from data loss to device management, multiple platforms and diverse applications... suddenly BYOD and mobility have become your problem.

And that's before you've factored in the significant increase in cybercrime targeted specifically at mobile devices and applications.

Today, Apple's iOS, OS X and Google's various flavours of Android operating systems are as prolific as Windows. In Q2 2012, the number of Trojans targeting the Android platform nearly tripled compared with the same period in 2011[4] (see fig 4).

This trend is set to increase, as the ease of which a business person's mobile data can be taken or intercepted makes mobility a new battleground for cybercrime.

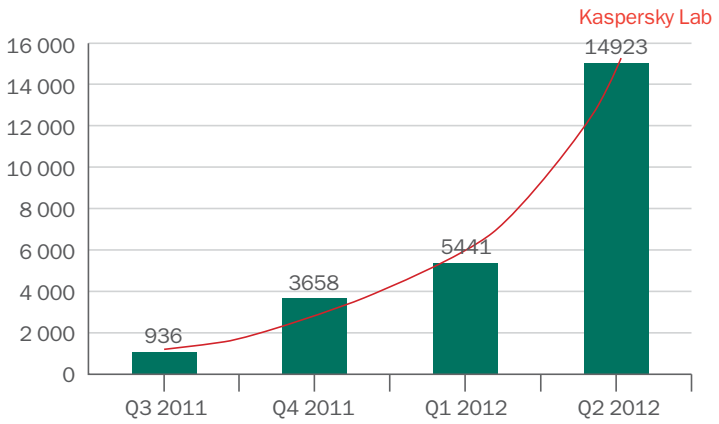
"BYOD is one of the biggest risks to IT security. Both in targeted and non-targeted attacks having personal devices on the network brings extremely difficult challenges. Ideally, personal and business use should be completely separated and segregated."

Roel Schouwenberg, Senior Security Researcher, Kaspersky Lab

CONSIDER...

- So how do you separate and protect business information on a user owned device and take advantage of the hardware savings BYOD can promise?
- How do you ensure that your employees' app habit doesn't become your network malware problem?
- How can you balance a key business requirement against security needs?

Fig 4: The number of malware modifications targeting Android OS



4. Source: securelist.com Q2 2012 report: http://www.securelist.com/en/analysis/204792239/IT_Threat_Evolution_Q2_2012

ENCRYPTION: UNDERSTANDING THE TRUE COST OF PROTECTING YOUR ASSETS.

6

Loss of hardware is a common issue for IT, this causes a number of headaches for you to deal with – not least the cost of replacing the device but also the more hidden challenge of ensuring sensitive company information is kept safe.

Factor in the ever-increasing range of government fines for data breaches, reputational damage and impact on customer loyalty, and it's easy to see how the costs of a data breach spread well beyond hardware replacement.

Using the example of a lost laptop at an airport, let's look at the true cost (and risks the broader business may not be aware of) when making sure your assets are protected.

In the United States alone, 12,00 laptops are left behind in airports every week.[1] That's 624,000 every year - amounting to an estimated $987 million in hardware costs alone. And that's just for one country. Imagine what the global figures could be – and that's not even the whole picture.[2]

There is a bigger financial impact which the broader business may not understand and that's the cost of data leakage.

In the US alone, data leakage costs an estimated $25 billion annually.

And 85% of people surveyed said they would take their business elsewhere if a company lost their data and 47% said they would take legal action.[3]

While encryption has traditionally been viewed as complex or expensive, it's no longer the case: this data protection technique is being embraced with 43% of enterprises encrypting all their data and 36% of small businesses encrypting highly sensitive data[4].

It may sound obvious, but unauthorised users and criminals can't read encrypted data. This makes encryption a core component of any Unified EPP.

"The rise in encryption is directly related to the growing realisation that 'always-on' staff, working any time, any place, anywhere and from any device, puts unencrypted data at greater risk than ever."

David Emm Senior Regional Researcher Kaspersky Lab.

Fig 5

1. Source: WBMF News October 2012 2. Source: Ponemon: The cost of a laptop April 2009 3. Source: Newspoll Survey November 2011 4. Source: Kaspersky Lab – Coping in the chaos Global IT Risk Report 2012

ENDPOINT SECURITY… WHAT ARE THE OPTIONS?

7

Option 1 – Anti-malware only

Strong, up-to-date anti-malware plays a central role in IT security. But on its own, it simply isn't enough to protect the business from targeted attacks using other methods, such as phishing and social engineering. And it definitely can't help you to manage your other security obligations and tasks.

Option 2 – Buy a one-size-fits-all packaged solution

Many available security solutions appear to offer a lot: you've got encryption, anti-malware, vulnerability scanning…pretty much everything you think you need to be secure. But what if you only want some functionality and not others? What if you don't need, say, MDM now, but you know business is planning a BYOD initiative next year – can you add that on later rather than paying for functionality you don't need today?

And do you really know what you have invested in? It might have arrived in the same box, but the reality is that many 'solutions' are the result of multiple bolt-on, bought-in solutions from other companies. These aren't always as compatible as they first appear, and can cause more problems than they solve if something goes wrong.

Option 3 – Assemble a selection of different solutions from different vendors and make them work together

There are many quality standalone solutions available. The problem is getting them to work together – and even when they do, you're left with the challenge of dependencies, multiple agents, multiple consoles, multiple maintenance requirements and multiple reports.

You can never really get the most out of everything each separate solution offers because they were never designed specifically to work together.

Complexity is the enemy of IT security. A 'single pane of glass' view of your entire security environment not only frees you up to spend time on other projects, but will give you a more comprehensive understanding of current – and future – security needs.

THE PROS AND CONS

All-in-one package

Pros: Seems less complicated, fewer licenses to manage, often less expensive than buying separate applications.

Cons: Often cobbled together from multiple business acquisitions and mergers – and lacking in genuine integration as a result.

Cons: Because it's one-size-fits all, you're often paying for functionality you don't yet need. This is particularly true of 'Small Business' versions – they're often just badly pared down enterprise editions, not genuinely scaled to requirements.

Use different vendors

Pros: You can pick and choose exactly what you need, when you need it.

Cons: Can be difficult to integrate with other solutions. Also adds to the complexity of your IT environment, potentially blurring the view.

Cons: More of your time spent managing multiple vendors

AT A GLANCE

- Anti-malware is no longer comprehensive or robust enough to fully protect businesses
- Packaged solutions are often 'bolted together' rather than truly integrated
- Best of breed works well, but is expensive and requires ongoing internal resource

ENDPOINT SECURITY – THE KASPERSKY OPTION.

8

Move beyond simply plugging the gaps and take a systems-wide approach to security and information protection.

Kaspersky Endpoint Security for Business gives you the building blocks you need to create the comprehensive endpoint protection platform you want whilst meeting your businesses needs.

SEE IT. CONTOL IT. PROTECT IT.

Imagine having one clear view of your entire IT environment, from network to device, data centre and desktop.

You get the total visibility you need to manage threats, the ability and flexibility to respond quickly to malware and the capacity to respond to the changing needs of the business, whether that's mobile device support or managing guest access on the network.

No bolt-on functions. No bought-in, cobbled together technologies…Just one code-base, developed in-house, designed to complement and enhance overlapping functionalities. All running from a single, easy-to-manage console.

From one solid, genuinely integrated platform, Kaspersky Lab allows you to exploit the commonalities between day-to-day systems management functions and key information security needs.

Fig 6

Kaspersky Endpoint Security for Business

All managed through a single management console:

Kaspersky Security Center

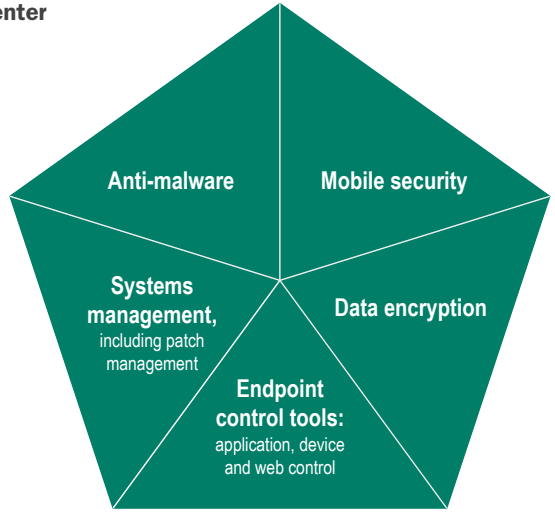


Fig 7

AT A GLANCE

- With Kaspersky Security for Business, delivering the industry's first true Security Platform built from the ground up.
- Making it easy for IT administrators within any size of organisation to see, control and protect their world, all from just one management console.
- Protect your company's data, no matter where it is, without adding to your resource requirements.
- An interface that's intuitive, and technology that's easy to use, easy to deploy and easy to manage.
- Reduce your business risk, and maintain maximum business efficiency.
- Scaleable, modular solution that can grow with your business and respond to change

With Kaspersky, Now You Can

Fig 8: Anti –malware – The starting point of the platform is Kaspersky's award-winning anti-malware technology. This technology consists of several scanning modules, cloud-assisted protection and a robust firewall. Central management is accomplished by Kaspersky Security Center. As new features are added, the additional management tools will also be accessed through this same console.

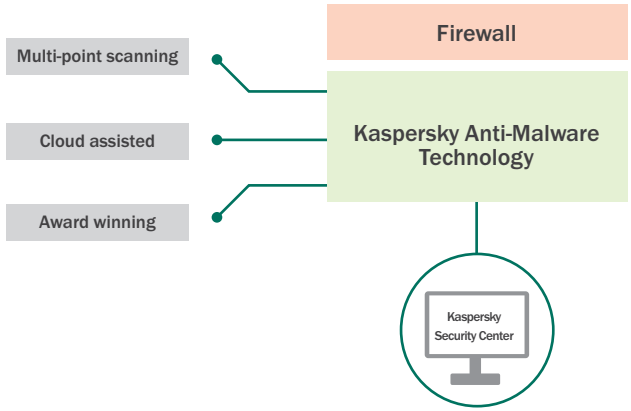


Fig 9: Mobile device management – Control, manage and secure company or employee-owned mobile devices and removable media from a central location. Support BYOD initiatives by exploiting containerisation features, remote wipe, encryption and other anti-theft functionality.

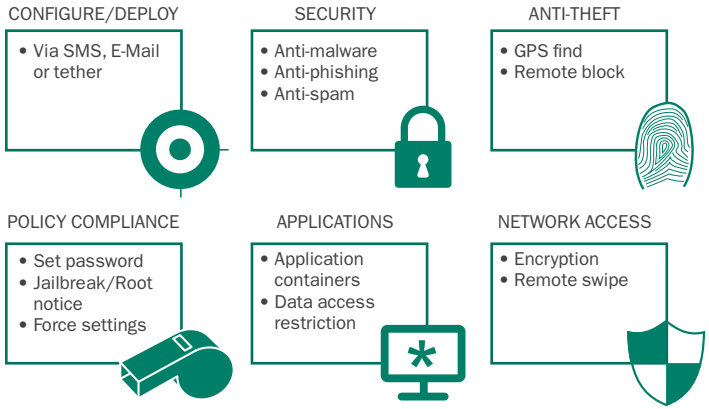


Fig 10: Encryption – Full Disk Encryption (FDE) and File Level Encryption (FLE), centrally managed. Automate enforcement, apply policies based on your unique needs – manage from one console.

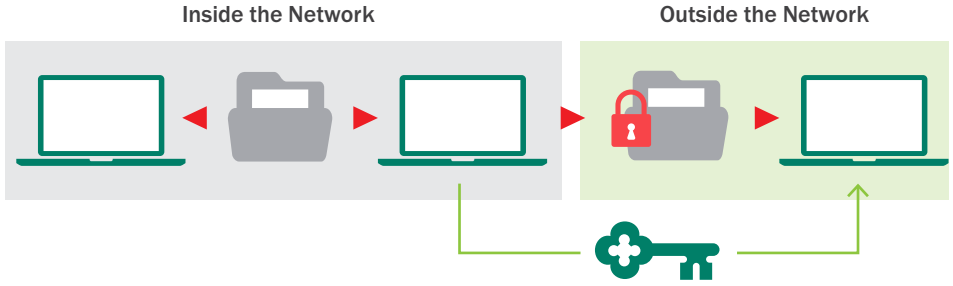
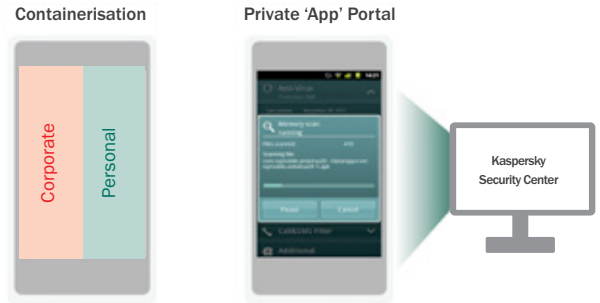


Fig 11: Systems Management and Control Tools – Automate and prioritise patch management, vulnerability scanning, image provisioning, reporting and other day-to-day management and control tasks. Merge day-to-day management and administration needs with information security requirements – enhancing security, reducing foot print and enabling you to focus on other projects.



- Keeps corporate data separate
- Encypted
- Selectively wiped

THE KASPERSKY OPTION – THE BUSINESS ARGUMENTS.

10

The evolving risk and threat landscape might be complex, but the approach needed is clear – as are the business benefits you can deliver to the rest of the organisation.

High detection rate equals reduced business risk

Kaspersky's exceptionally high detection rates mean the business is exposed to less risk. You face fewer malware incidents and achieve greater data protection – from both insider and outside risk.

Keeping your business data safe

The Payment Card Industry Data Security Standard (PCI DSS) specifically requires anti-virus on the desktop. Effective IT security is a core component of any regulatory compliance initiative. Many industry sectors now mandate encryption as a standard part of data protection compliance; even if your jurisdiction doesn't require it, increasing customer awareness of data breach risk has transformed encryption into a key competitive advantage.

Say yes to mobility

No need to view changing technologies and work practices with suspicion. Kaspersky Lab's MDM functionality means you can say yes to BYOD device or mobile work initiatives without exposing the business to additional risk.

Increased productivity

Integrated security relieves pressure on resources: fewer staff are needed to constantly monitor, define, maintain and report. Mining data logs and other information from a single, integrated solution is also far easier than attempting to slice and dice data from multiple, semi-compatible systems.

Better visibility equals better management

One management console gives your business complete visibility across virtual, physical and mobile endpoints. As soon as a new device is introduced to the network, you're made aware and your policies automatically applied.

AT A GLANCE

- High detection rate equals reduced business risk
- Keeping your business data safe
- Say yes to mobility
- Increased productivity and greater insight
- Better visibility equals better management

TAKING THE CONVERSATION WIDER – BUILDING A BUSINESS CASE.

11

Key elements for building a robust business case for IT security investment

While every business is unique, Kaspersky Lab has found the following to be significant points for discussion:

1

Do highlight the risks upfront, but don't focus on Fear, Uncertainty, Doubt (FUD)

The statistics about the rise of IT security risks are very compelling, as they show a trend of both volume (more threats, more quickly) and complexity (targeted attacks and greater sophistication of malware). However, this in itself is not a business case, and the IT industry has historically been guilty of using fear to sell. A cynical Finance Director or CEO will have heard the scare stories before and usually see them as marketing hype.

2

Position IT security as a business enabler, not inhibitor

It is a far better strategy to focus on how IT security is actually a business enabler. Proper security and security controls allow businesses to implement innovative technologies and working methods – safely.

3

Mobility and BYOD are critical for the business, show that IT security must be a part of this

As a logical extension of the previous point, mobility and BYOD are key areas that the business is looking to harness for productivity value, but also where IT security is absolutely essential. Key here is that employees (many of them senior employees) will be carrying potentially sensitive and/or valuable company data. Securing this data is far more important than the value of the device itself, and data encryption and MDM are both essential tools for any mobile-enabled business.

4

Platforms win on efficiency and productivity – so analyse what your return will be

Endpoint protection platforms allow you to see, control and protect all your endpoints, from one place. What this means is that you will need to spend less time on the monitoring and management of your IT security, and changes, updates and patches can be carried out once, rather than through multiple systems. This time-saving cannot be under-estimated and some basic analysis will give you a meaningful figure to include in your business case. Obviously the cost of buying multiple systems will also be a factor, but the human time cost is a greater factor and one that productivity-focused management teams will empathise with.

To find out more, visit
www.kaspersky.com/business

ABOUT KASPERSKY LAB

Kaspersky Lab is the world's largest privately held vendor of endpoint protection solutions. Throughout its 15-year history Kaspersky Lab has remained an innovator in IT security and provides effective digital security solutions for consumers, SMBs and enterprises. The company currently operates in almost 200 countries and territories across the globe, providing protection for over 300 million users worldwide. Learn more at www.kaspersky.com.

KASPERSKY lab